A Game-Theoretic Approach to Network Security

Mohammad Pirani and Henrik Sandberg

Department of Automatic Control
KTH Royal Institute of Technology

Outline

- Defense mechanisms in cyber physical systems security
- Game-theoretic approach to the visibility-impact trade-off
- Game-theoretic approach to maximizing the attack energy
- Conclusion and future directions

1. M. Pirani, E. Nekouei, H. Sandberg, K. H. Johansson, “A game-theoretic framework for security aware sensor placement problem in networked control systems", *Proceedings of ACC 2019, the 38th American Control Conference*, Philadelphia, USA, 2019 (to appear).

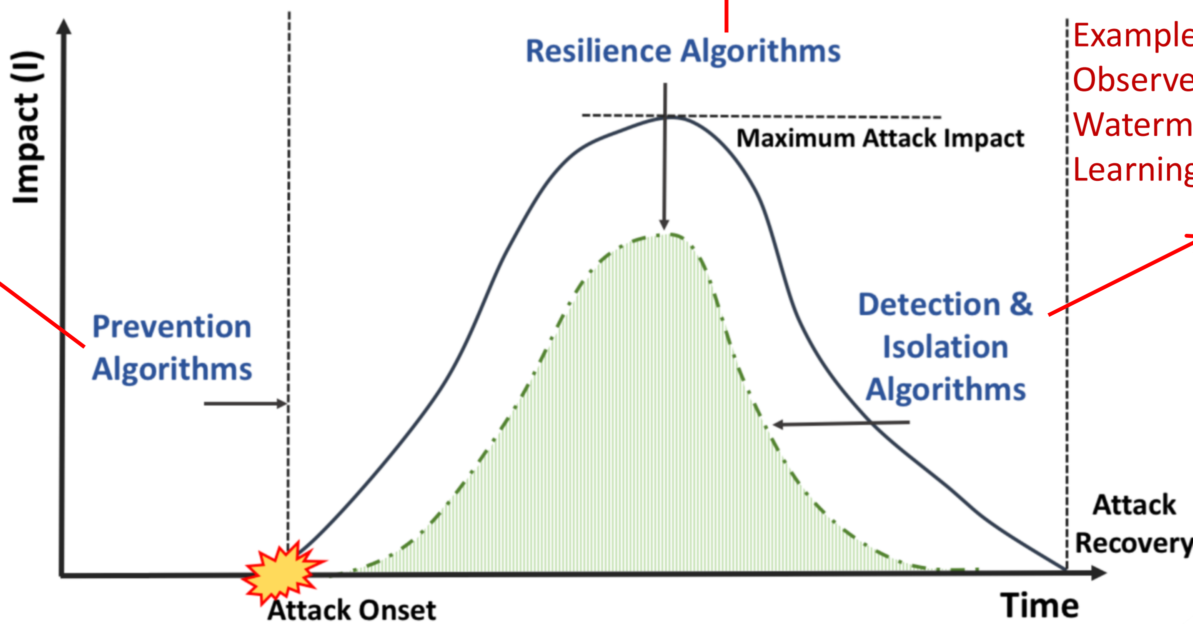
2. M. Pirani, E. Nekouei, S. M. Dibaji, H. Sandberg, K. H. Johansson, " Design of Attack-Resilient Consensus Dynamics: A Game-Theoretic Approach", *Proceedings of ECC 2019, the 17th European Control Conference, Naples, Italy, 2019 (to appear)*.

Defense Mechanisms

We classify various defense mechanisms into three major classes: **prevention**, **resilience**, and **detection**.

Examples:
Robust control methods/ event triggered control
Game-theoretic methods
Trust-based approaches

Examples:
Cryptography
Randomization



Examples:
Observer-based methods
Watermarking
Learning-based anomaly detection

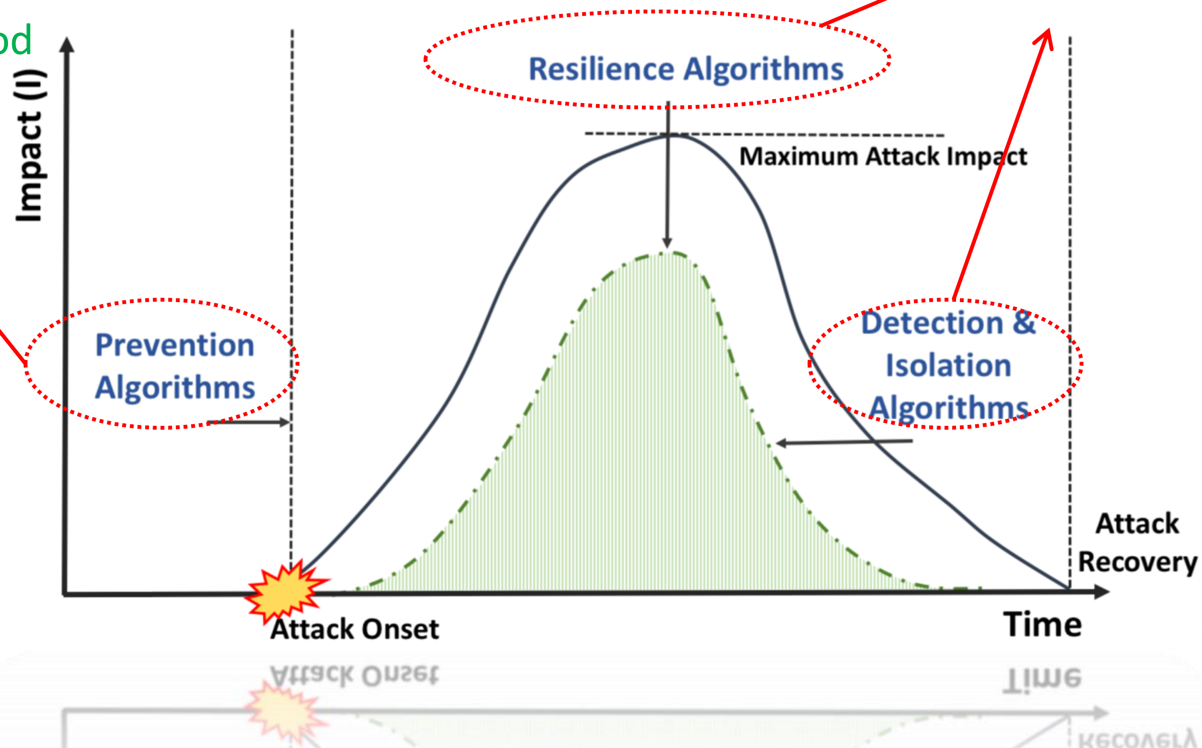
Dibaji, Pirani, Johansson, Annaswamy, Chakrabortty "Annual Reviews in Control", 2019, to appear.

A Game-Theoretic Approach to Network Security

- We adopt some game-theoretic approach in addressing these three defense mechanisms.

We investigate the **trade-off** between **Impact** and **visibility** for the attacker.

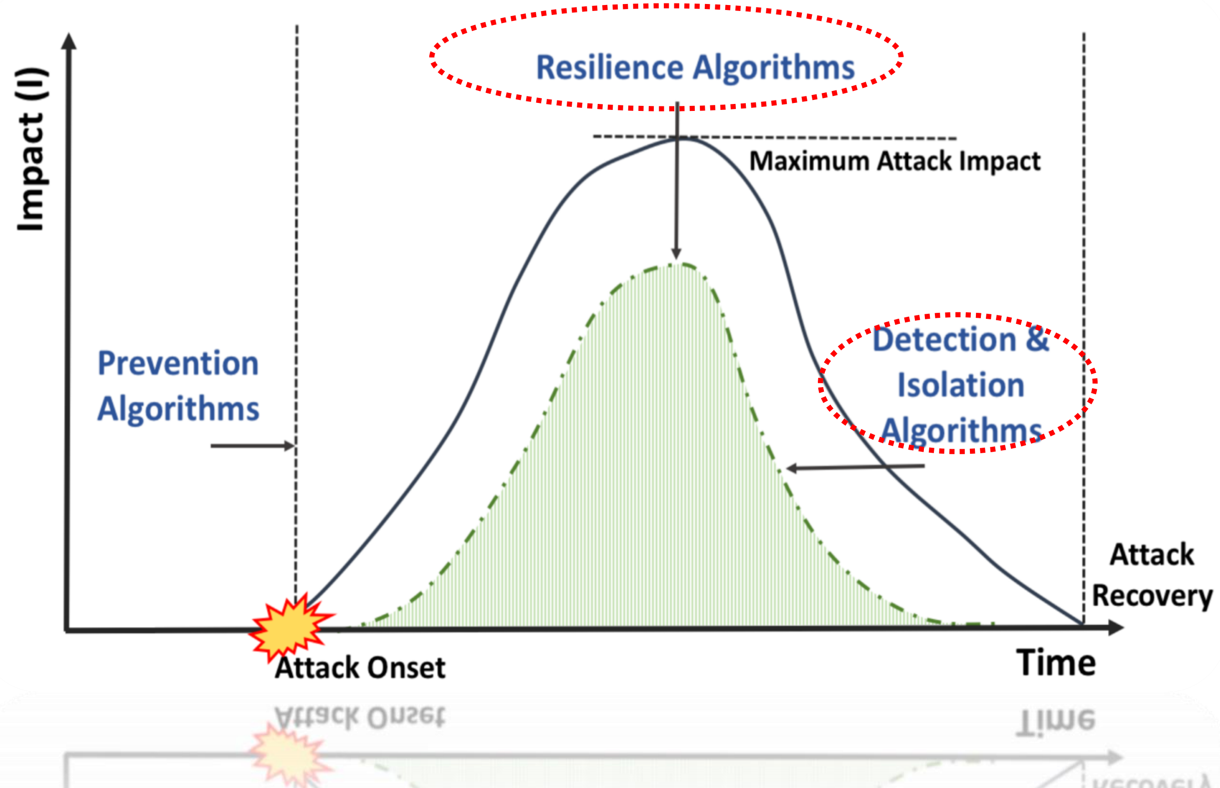
We discuss a method to **increase the cost** of the attack.



Problem 1: Trade-off between visibility and impact

Objective:

- To investigate the trade-off between **visibility** and **impact** (from the attacker's perspective).



Statement of Problem 1

- There is an attacker which tries to attack some nodes:

1. To have (**large**) **impact** on a targeted node,
2. Remains **covered (as much as possible)** to a set of detectors.

- There is a detector which aims to detect the attack signals as much as possible

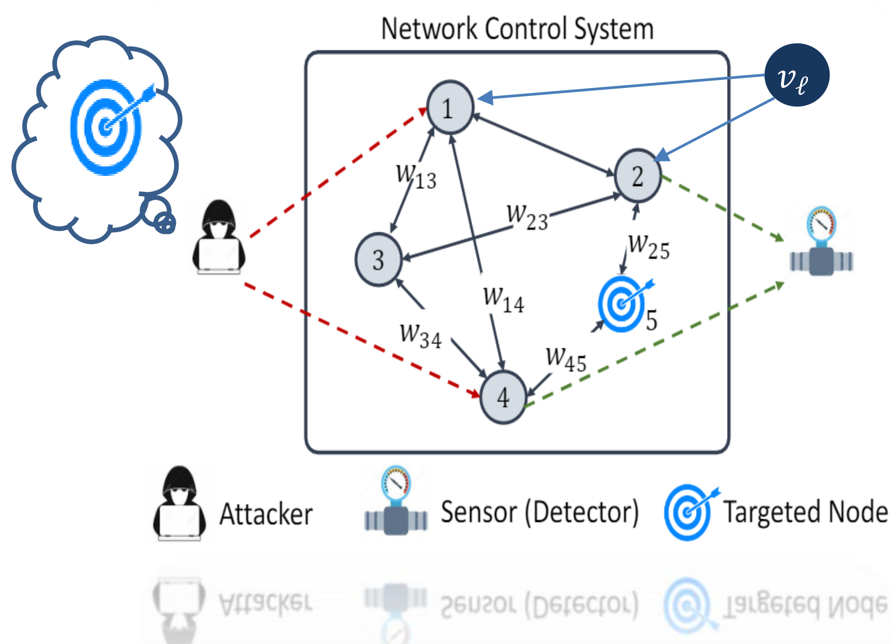
We focus on leader-follower dynamics

$$\dot{x}(t) = Ax(t) + Fu(t) + Bw(t)$$

$$y(t) = Cx(t)$$

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}^T$$ Attacker's decision

$$C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$ Detector's decision

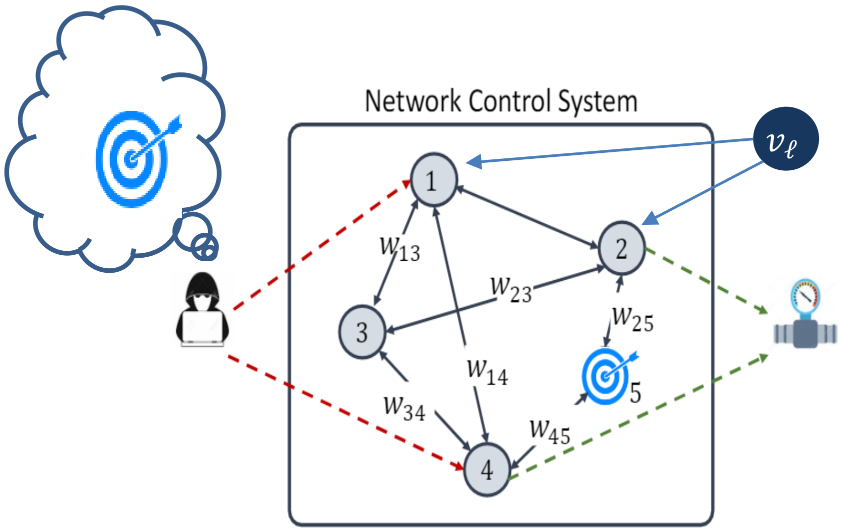


Statement of Problem 1

- The way we quantify attack impacts on targeted node and on the sensor is via system norms.

System norm from the attack signal $w(t)$ to the output of interest:

$$||G||_\infty = \sigma_{max}(C^T A^{-1} B)$$



Game objective:

$$J\_attack = \min_{B} \sigma_{max}(C_{detect}^T A^{-1} B) - \lambda \sigma_{max}(C_{target}^T A^{-1} B), \lambda \geq 0$$

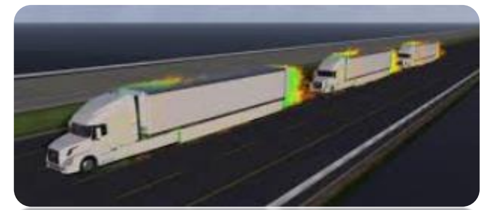
$$J\_defender = \max_{C_{detector}} \underbrace{\sigma_{max}(C_{detect}^T A^{-1} B)}_{visibility} - \lambda \underbrace{\sigma_{max}(C_{target}^T A^{-1} B)}_{Impact}, \lambda \geq 0$$

Applications

- Formation of autonomous

$$m_i \ddot{x}_i = \sum_{j \in \mathcal{N}_i} k_{ij}\left(x_j - x_i\right) + c_{ij}\left(\dot{x}_j - \dot{x}_i\right) + w_i(t),$$

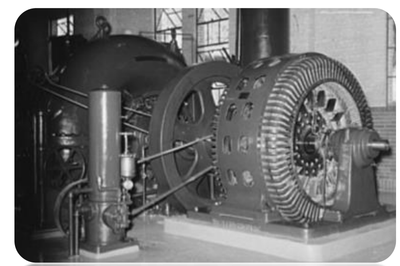
Force | Distance | Rel. Velocity | External attack



- Voltage control in power grids:

$$m_i \ddot{\theta}_i + c_i \dot{\theta}_i = P_{m,i} - P_{e,i} + w_i(t)$$

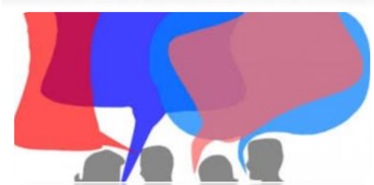
Frequency | Mechanical and Electrical powers | External attack



- Opinion Dynamics in the presence of stubborn

$$\dot{\psi}_j(t) = \sum_{v_i \in \mathcal{N}_j} (\psi_i(t) - \psi_j(t)) - k_j(\psi_j(t) - \psi_j(0)) + w_j(t).$$

Level of Stubbornness



Detectability-Impact Tradeoff

- What is the effect of λ on the game value J^* and game strategies?
- Parameter λ characterizes the **domination** of **visibility** with respect to the **impact**.

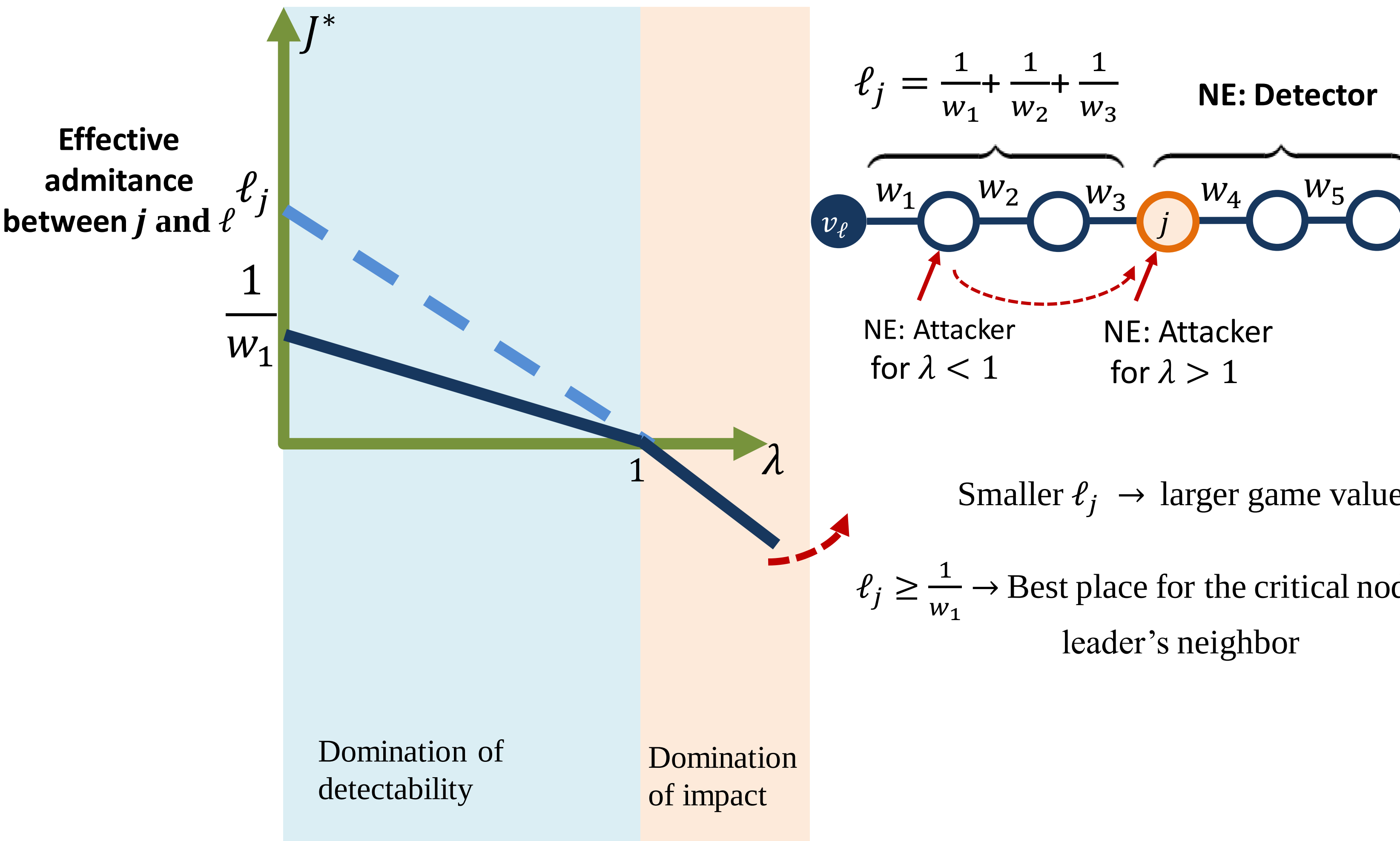
Game objective:

$$J = \min_{B} C_{detect}^{T} A^{-1} B \; - \lambda C_{target}^{T} A^{-1} B \;\; , \lambda \geq 0$$

$$J = \max_{C_{detector}} \underbrace{C_{detect}^{T} A^{-1} B}_{Detectability(visibility)} \; - \lambda \underbrace{C_{target}^{T} A^{-1} B}_{Impact} \;\; , \lambda \geq 0$$

Visibility-Impact Tradeoff: Undirected Trees

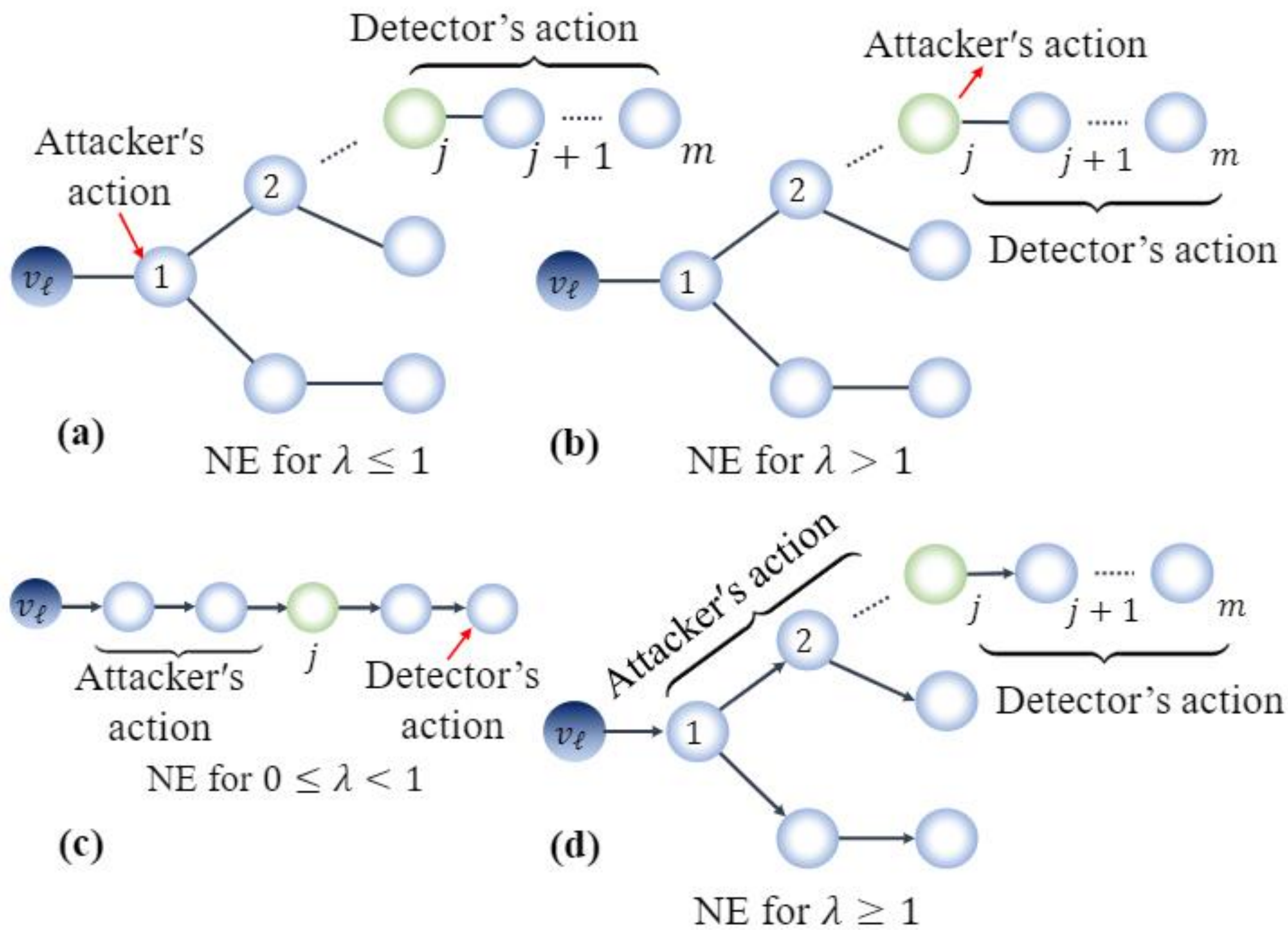
Game Value J^* vs λ for Undirected Trees



Smaller ℓ_j → larger game value

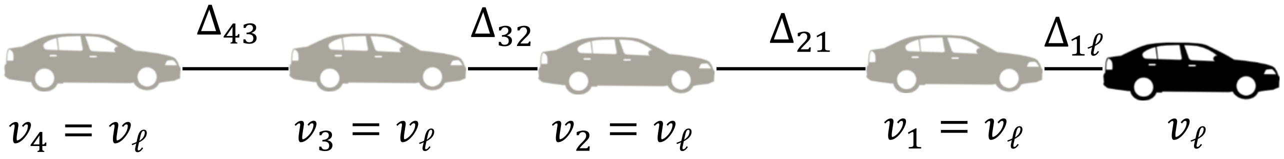
$\ell_j \geq \frac{1}{w_1}$ → Best place for the critical node is the leader's neighbor

NE Strategies for Undirected and Directed Trees



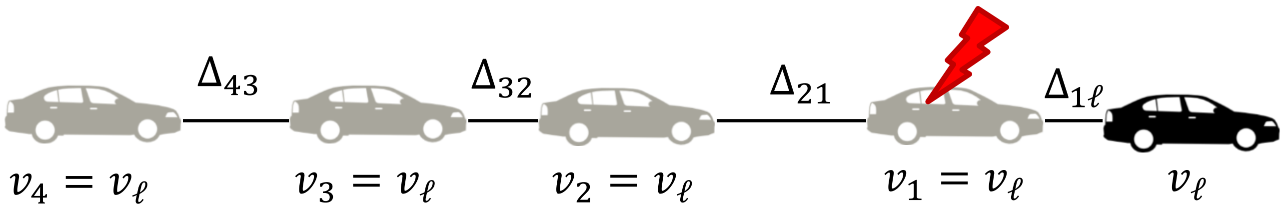
Applications to Secure Vehicle Platooning

- Consider a network of connected vehicles.
- Each vehicle tends to track a **particular velocity** (introduced by the leader), while remains in a **specific distance** from its neighbors.



Secure Vehicle Platooning - Dynamics

- Consider a network of connected vehicles.
- Each vehicle tends to track a **particular velocity** (introduced by the leader), while remains in a **specific distance** from its neighbors.



$$\ddot{p}_i(t) = \sum_{j \in N_i} k_p\big(p_j(t) - p_i(t) + \Delta_{ij}\big) + k_u\Big(u_j(t) - u_i(t)\Big) + w_i(t)$$

Position of v_i

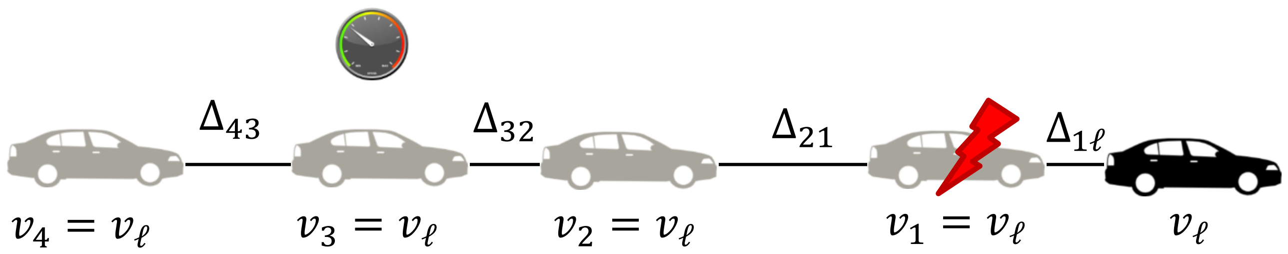
Desired inter-vehicular distance

Velocity of v_i

Attack signal

Dimension: acceleration

Secure Vehicle Platooning - Dynamics



$$\dot{\boldsymbol{x}}(t) = \underbrace{\begin{bmatrix} \mathbf{0}_n & I_n \\ -k_p L_g & -k_u L_g \end{bmatrix}}_{A} \boldsymbol{x}(t) + \underbrace{\begin{bmatrix} \mathbf{0}_{n\times 1} \\ k_p \boldsymbol{\Delta} \end{bmatrix}}_{B} + \underbrace{\begin{bmatrix} \mathbf{0}_n \\ B \end{bmatrix}}_{F} \mathbf{w}(t),$$

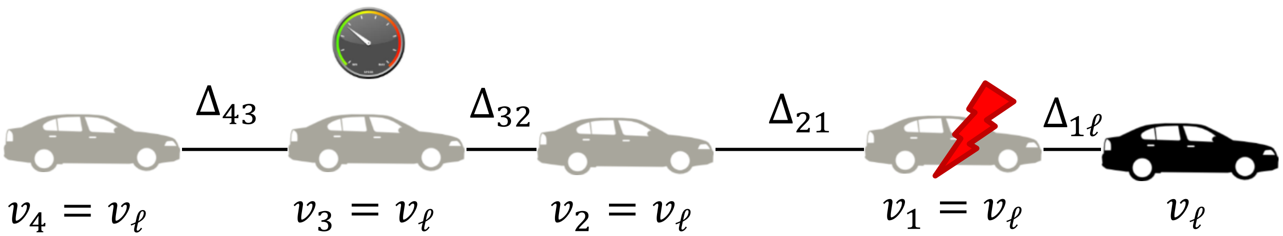
Attack signal

$$\boldsymbol{y}(t) = [\mathbf{0}_n \quad C]\boldsymbol{x}(t)$$

Sensor measurements: velocities

Matrices B and C are similar to what was defined previously.

Secure Vehicle Platooning - Dynamics



$$\dot{\boldsymbol{x}}(t) = \underbrace{\begin{bmatrix} \mathbf{0}_n & I_n \\ -k_p L_g & -k_u L_g \end{bmatrix}}_{A} \boldsymbol{x}(t) + \underbrace{\begin{bmatrix} \mathbf{0}_{n\times 1} \\ k_p \boldsymbol{\Delta} \end{bmatrix}}_{B} + \underbrace{\begin{bmatrix} \mathbf{0}_n \\ B \end{bmatrix}}_{F} \mathbf{w}(t),$$

$$\boldsymbol{y}(t) = [\mathbf{0}_n \quad C]\boldsymbol{x}(t)$$

L_2 gain from $w(t)$ to $y(t)$= $-CA^{-1}B = \frac{\mathbf{1}}{\boldsymbol{k_p}} \boldsymbol{C L_g^{-1} B}$

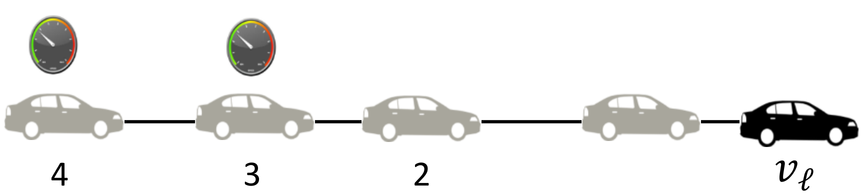
Equilibrium Analysis for Symmetric Platooning

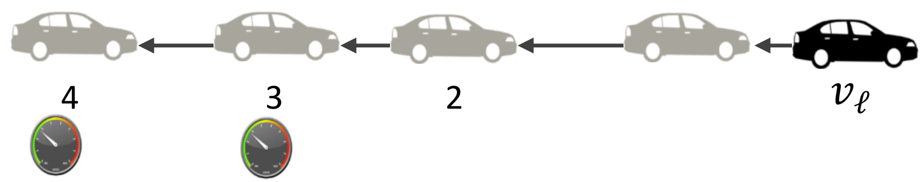
Theorem: For a leader-follower vehicle platoon under f attacks and f detectors both **directed and undrected networks**, there exists an equilibrium which happens when the detector places f sensors in the **farthest nodes** from the leader.

Attacker should solve an optimization problem to find its best strategy.

It is computationally hard, but it is the attacker's business!

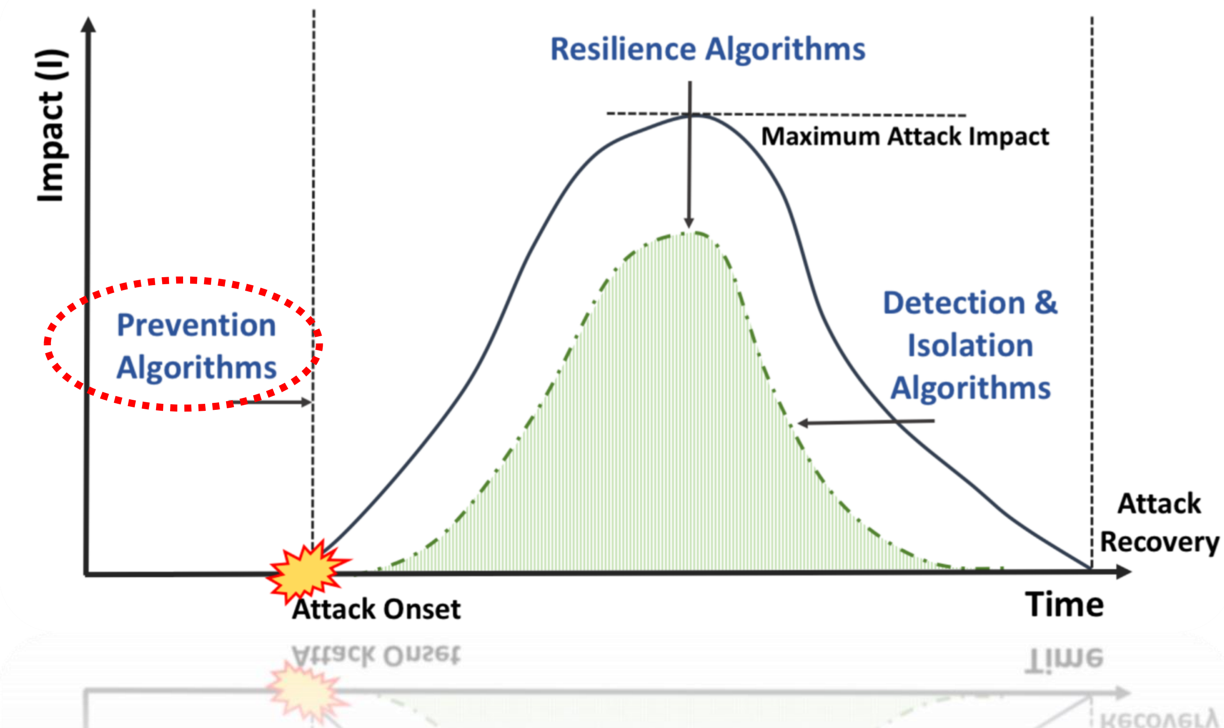
Remark: The game value for directed graphs is smaller than that of undirected graphs.





Problem 2: Prevention

- A Prevention approach is to increase the cost (**energy**) of the attack.
- Previous methods usually demand a **large graph connectivity.**



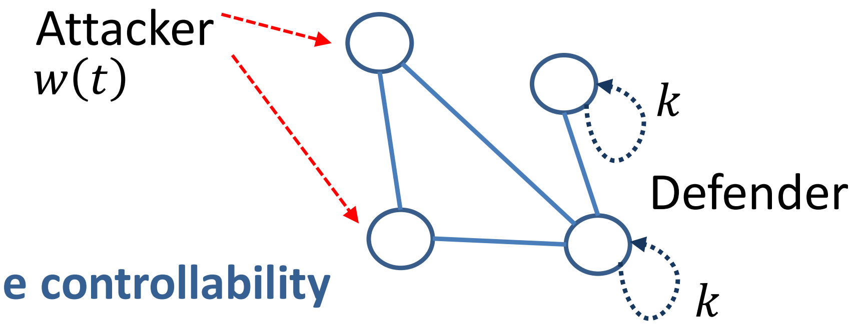
Statement of Problem 2

- There is an attacker which targets some nodes to **steer** the consensus dynamics into its desired direction **with minimum energy**, and a defender which tries to maximize this energy.

$$\dot{x}(t) = (A + \boldsymbol{B}K)x(t) + \bar{\boldsymbol{B}}w(t)$$

Defender's action

Attacker's action



This **energy** is characterized via the **trace of the controllability Gramian**, obtained by solving the Lyapunov equation.

Game objective:

$$J\_defender = \min_{B} trace\ (\bar{B}^T(A + BK)\bar{B})$$

$$J\_attacker = \max_{\bar{B}} trace\ (\bar{B}^T(A + BK)\bar{B})$$

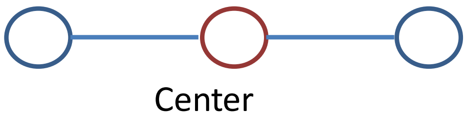
This game does not admit a NE.

We adopt a Stackelberg game strategy (defender is the leader).

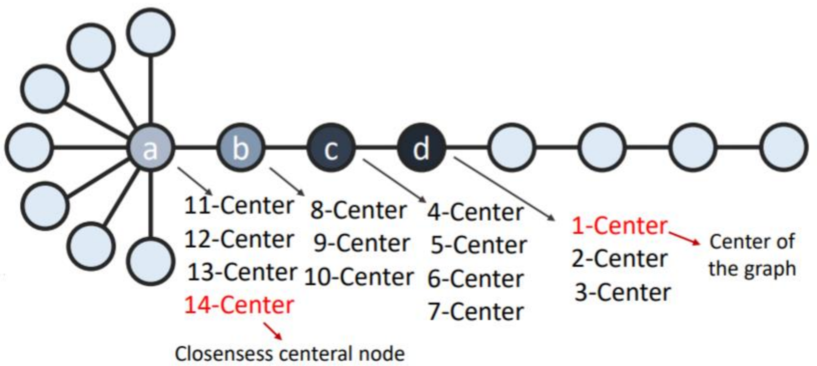
Optimal Placement of Defenders

- What does the equilibrium of this game tell us about the locations of defender nodes?

Definition (Graph Center): The center of a graph is a set of vertices whose maximum distance from any other node in the network is minimum.

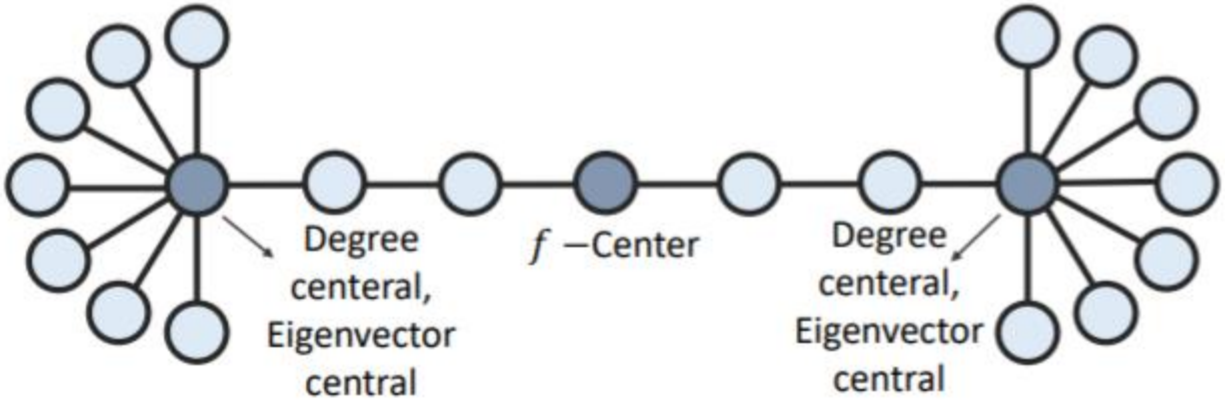


Definition (Graph f −Center): The f −center of a graph is a vertex whose maximum summation of distances to any combination of f nodes in the network is minimum.



Optimal Placement of Defenders

- **Theorem:** a solution of the game is when the defender chooses the weighted f −center of the graph and the attackers choose the farthest f nodes from the f −center.



The graph f −center can be arbitrarily different from degree based centralities.

- ✓ For general undirected graphs, the distance between two nodes is replaces with their effective resistance.
- ✓ The above theorem will hold, only replace f −center with effective f −center.

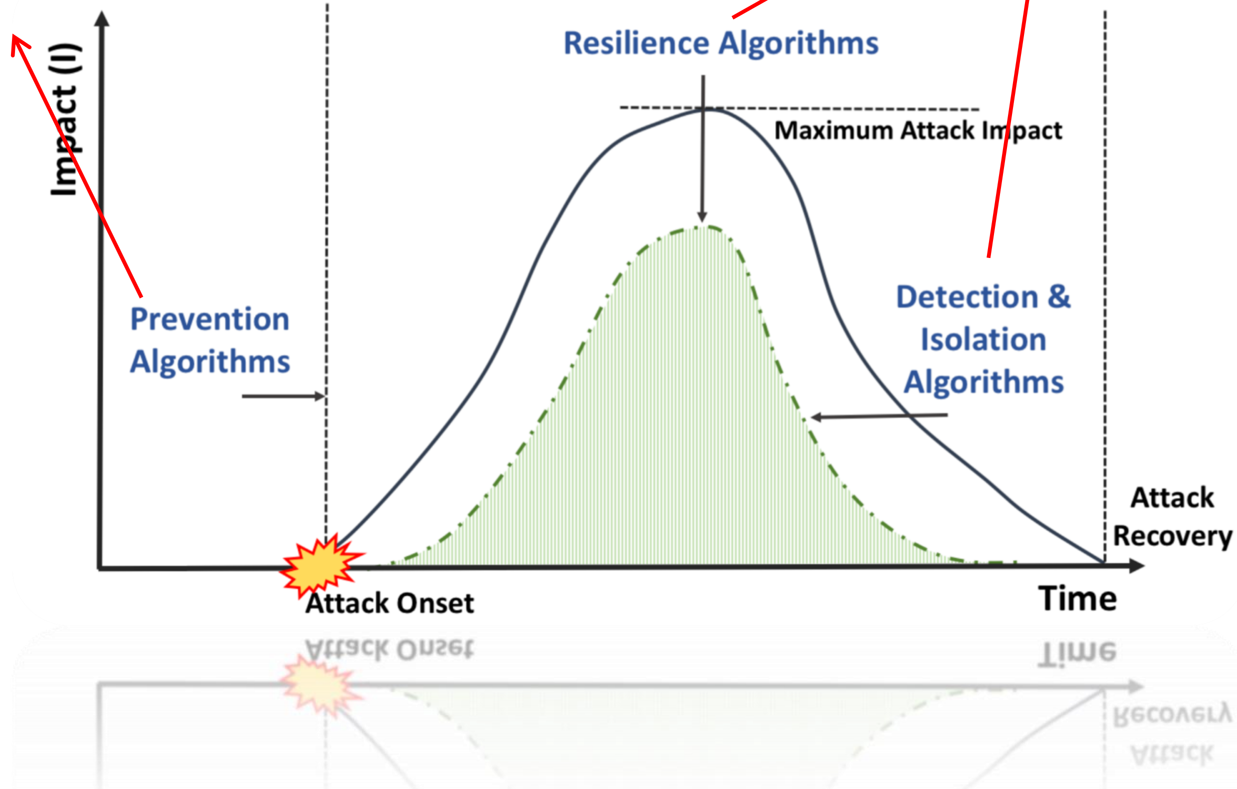
Summary

Trade-off between

Impact, visibility, and robustness.

Energy maximization

Via controllability Gramian for the attacker



Future Direction

- To extend the theoretical results to capture **more general dynamical systems** on **more general graph topologies**.

Thank You